Diary of Mathematical Musings

Patrick Stein

Contents

CHAPTER 1

2002-08

2002-08-15 08:48:06—P = NP

There is a question as to whether $P = NP$, where P is the set of decision problems for which there is a deterministic algorithm that runs in a number of steps bounded by a polynomial function of the size of the input and NP is the set of decision problems for which there is or is not a deterministic algorithm in P yet there is an algorithm in P with which to verify any proposed solution. The question of whether $P = NP$ amounts to the question of whether there are any decision problems for which a proposed solution can be checked in P but for which there can be no algorithm in P which will guarantee a solution.

There is also a class of decision problems called NP-complete. This class of problems has been shown to be as hard as NP can get. That is to say, if one could show that the NP-complete problems are P, then $P = NP$. Additionally, it has been proven that all NP-complete problems are equivalent, in the sense that if one showed that one NP-complete problem was in P, then all of the NP-complete problems would be in P.

Someone mentioned today in the mathematics community on livejournalthat the question may be formally undecideable. I have never considered that possibility before. That is, it may be impossible to prove or disprove $P = NP$ with the relevant set of axioms.

I'm not sure what the relevant axioms are, actually. I'm sure they are entwined with Turing machines or lambda calculus and probably have enough other stuff tacked on to actually be able to distinguish things which can be bounded by polynomials from things which cannot be bounded by polynomials. If the axioms don't stretch that far, then it is clear[1] that they'll never be able to prove or disprove the statement.

I know that the Axiom of Choice (AC) in Axiomatic Set Theory was shown to be unproveable from the other axioms by Gödel. Later, Cohen proved that the negation of the Axiom of Choice ($\overline{\text{AC}}$) is also unproveable from the other axioms. Obviously, if could be proven, then it would be a Theorem instead of an Axiom. And, similarly if its negation would be proven, then we'd toss out AC.

Things are quite similar for Euclid's Fifth Postulate. It is consistent with the first four postulates to either affirm or deny the fifth. As such, the fifth is neither a Theorem or excised.

Geometry has handled this better than Set Theory handled AC. Geometry has gone on exploring various alternatives to the Fifth Postulate. Rather than expending huge amounts of effort to rid all proofs of their dependence on a particular

[1] Assertion

variant of the Fifth Postulate, they've just accepted the fact that they have to specify which variant of the Fifth Postulate they're depending upon.

Set Theory, on the other hand, has tried to prove every theorem which depends upon the Axiom of Choice in some way which doesn't require it. This hasn't been a very successful venture. But, there are still thousands of mathematicions who are very leary of it. At the same time, I don't think many mathematicians have ever come up with a serious proposition that depends on $\overline{\mathrm{AC}}$.

I don't really know how computational theory has handled the possiblity that $P = NP$ may not be formally decideable. No one has yet proven that it is unproveable or that its negation is unproveable, so maybe it's jumping the gun a little bit.

At the moment, I seem to be at a loss for terminology. I'm going to enumerate the possible relationships between a set of axioms and a new proposition. Then, I'll try to see what terminology I've got.

(1) The axioms imply the proposition.
(2) The axioms imply the negation of the proposition.
(3) The axioms imply neither the proposition nor the negation of the proposition.
(4) The axioms imply both the propostion and the negation of the proposition.
(5) The axioms plus the proposition make a consistent system.
(6) The axioms plus the negation of the proposition make a consistent system.
(7) The axioms plus the proposition make an inconsistent system.
(8) The axioms plus the negation of the proposition make an inconsistent system.

By inconsistent, I mean that one could prove some statement and its negation with the system. By consistent, I mean that no statement which was proveable with the axioms is disproveable with the axioms plus the proposition.

If 1 holds, then the proposition is a theorem. If 2 holds, then the negation of the proposition is a theorem. If 3 holds, then the proposition is independent of the axioms. If 4 holds, then the axioms are inconsistent and should be tossed. If 5 holds, then xeither 1 xor 3 must hold. If 6 holds, then xeither 2 xor 3 must hold. If 7 holds, then xeither 2 xor 4 must hold. If 8 holds, then xeither 1 xor 4 must hold.

Option 2 could also be stated: The axioms deny the proposition. Similarly, "deny" could take the place of "imply the negation of" in 3 and 4, as well.

So, I guess there is enough vocabulary.

But, now I should be more clear about AC and Euclid's Fifth Postulate. With respect to the Zeremelo-Frankel Axioms of Set Theory, the proposition AC is 3, 5, and 6. With respect to Euclid's first four postulates, the proposition of his fifth postulate is 3, 5, and 6.

It is still unclear where the proposition $P = NP$ stands with respect to whatever axiom set is used for meta computational complexity problems. However, it would only take one P algorithm that deterministically solves one NP-complete problem to show that $P = NP$ is 1 and 5 but not 2 or 3 or 6 or 7 or 8.

2002-08-15 10:05:38—Well-ordering the reals with the surreals

I was pondering earlier this evening whether the surreal numbers provide a well-ordering of the real numbers. The surreal numbers are well-ordered. The real numbers are a subset of the surreal numbers. Where is the barrier? Is it that there can be so many surreal numbers between every real number? Is it that one reaches some limit-points (e.g. ω) before one gets all of the reals? Or, is it just that there is a problem on day ω in picking the largest (or smallest) number from the set of numbers born that day? I should ponder this one some more.

2002-08-16 01:36:40—Prime Certification in P

There's a new paper out that describes a polynomial-time algorithm for prime certification. I'm really going to have to take a look at it more closely. If there are some ways to exploit a similar technique for factorization, then I would have to hurry because I'm sure there's a flood of people looking into it now and before it made it to pre-print.

2002-08-16 16:15:54—Prime Certification in P

At first reading of their algorithm, it's not looking too promising that one could use it to find the factors of a composite number. But, there is still more to look for there.

2002-08-16 22:23:33—Pinching Factors

Consider trying to factor the number n. Clearly,

$$\lfloor\sqrt{n}\rfloor \cdot \left\lfloor\frac{n}{\sqrt{n}}\right\rfloor \leq n \leq \lceil\sqrt{n}\rceil \cdot \left\lceil\frac{n}{\sqrt{n}}\right\rceil \tag{1}$$

So, letting $a_0 = \lfloor\sqrt{n}\rfloor$ and $b_0 = \left\lfloor\frac{n}{a_0}\right\rfloor$, then clearly

$$a_i \cdot b_i \leq n \tag{2}$$

for $i = 0$. Similarly, letting $c_0 = \lceil\sqrt{n}\rceil$ and $d_0 = \left\lceil\frac{n}{c_0}\right\rceil$, we have

$$n \leq c_i \cdot d_i \tag{3}$$

for $i = 0$.

Our goal is to iteratively generate new a_i, b_i, c_i, d_i so as to pinch the gap between $a_i \cdot b_i$ and $c_i \cdot d_i$ while keeping n between them until equality is achieved in either equation 2 or equation 3.

I was hoping to be able to take products of $\left\lceil\frac{a_i}{2}\right\rceil$ or $\left\lceil\frac{b_i}{2}\right\rceil$ along with $\left\lfloor\frac{c_i}{2}\right\rfloor$ or $\left\lfloor\frac{d_i}{2}\right\rfloor$ to tighten the bounds. But, it gets stuck.

$$\begin{aligned} 7 \cdot 7 \leq & 55 \leq 8 \cdot 7 \\ 7 \cdot 7 \leq 4 \cdot 13 \leq & 55 \leq 8 \cdot 7 \leq 19 \cdot 3 \end{aligned}$$

Further iterations on the inner bounds do not help out at all, they only send us back to previously known states. If I do not stick to the innermost bounds then I'm no better off than just guessing.

2002-08-21 20:16:23—Finding Isomorphisms

In the LiveJournal Mathematics community today, someone asked about how to find isomorphisms. He was doing things with the five-element, idempotent, commutative quasigroups. The only tool that I had to use to find isomorphisms between them was brute force searching for one. There has to be a better way. That's a tool that I need.

Just for future reference, a quasigroup is a set of elements together with a multiplication operator. The multiplication operator $\circ$ need not be commutative or associative. But, it must be such that for any elements a and b, there is one and only one solution to $a \circ x = b$ and one and only one solution to $x \circ a = b$.

2002-08-27 01:39:15—Number Theory Outline

Someone created a LiveJournal community called `math_class`. I'm going to start doing some number theory lectures. I've pulled out some text books, but I'm not sure how much of an outline I should put together yet. I suppose we shall see.

2002-08-28 04:21:44—Oi...

I finally got my `math_class` introduction posted to LiveJournal. I spent way too long this evening making icons for it so that I could keep the lectures on my homepage, too. Urgle. Anyhow, it's just about bedtime now.

CHAPTER 2

2002-09

2002-09-10 14:47:26—Wheee...

I haven't written here in awhile. I ahven't even been thinking all that much math except for getting the Number Theory lectures up on LiveJournal..

Someone mentioned Geometric Algebra again yesterday. Oi, there are so many things that I want to learn.

I should mail back the professor at the UofM. And, before I go to see him, I should ponder a bit more about how Topology may be the next important math to hit Economics.

2002-09-12 20:14:15—Elliptic Curves

My copy of Koblitz's *Introduction to Elliptic Curves and Modular Forms* arrived today. I should work on my `math_class`, but I must read a chapter or two first.

CHAPTER 3

2002-10

2002-10-04 16:06:23—Equivalence Classes

I was reading Richard's course notes for Quantum Mechanics. He was talking about "ket space" and "bra space" and such. They are both complex vector spaces. I believe they are, techinally, complex projective spaces. Two vectors with the same direction are considered equivalent despite their magnitude.

I was trying to think about how this related to some of the other mathematical notations used when describing equivalence classes. For example, the integers modulo n is written both $\mathbb{Z}_n$ or as $\mathbb{Z}/n\mathbb{Z}$. The latter notation implies that there is homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$ with kernel $n\mathbb{Z}$. Further, it implies that there is only one such homomorphism.

We run into problems if we try to call this a homomorphism:

$$\sigma(\vec{a}) = \begin{cases} \vec{\emptyset} & ; \text{if} x = \emptyset \\ \left(\frac{1}{\sqrt{\vec{a}\cdot\vec{a}}}\right)\vec{a} & ; \text{otherwise} \end{cases}$$

The trouble is this:

$$\sigma(\vec{\emptyset}) \neq \sigma(1 \cdot \vec{a} + (-1) \cdot \vec{a}) \tag{4}$$

The topological notation doesn't quite work either. When one generates X/Y where $Y \subset X$, the implication is that all of the elements of Y are now just one element in the new space. It doesn't extend so much to the rest of the points. So, even if ℓ where some line through the origin (minus the origin), saying E^n/ℓ topologically would mean that the line (aside from the origin) has become a single point. Other lines through the origin could still be lines.

Actually though, the topological notation, along with preserving the vector-space structure may be enough here, I don't know. I think the topological notation could imply any of an infinite number of answers. But, the preservation of the vector space structure for the non-zero vectors may be enough.

Another possibility, I suppose is that, instead, we assume that the vectors form a vector space over S^1 instead of over $\mathbb{C}$. This doesn't really work though because $c_1\vec{a} + c_2\vec{a} \neq (c_1 + c_2)\vec{a}$ unless we define addition on S^1 pretty interestingly (which, I suppose we probably can). We can define the sum of points on the unit circle to be the normalized sum of the points on the unit circle. And, we can define the product of points on the unit to be their complex product. I think this still runs into the same problem the other homomorphism did though. It seems that to identify antipodal points on S^1, one has to do that first or else work in some very weird $E^2 - \{\emptyset\}$ thing that isn't quite a vector space.

CHAPTER 4

2003-10

2003-10-20 01:23:44—Equivalence Classes (revisited)

Wheee... it's been over a year since I've touched this. Lately, I've been updating `http://cayley.dyndns.org/twiki/bin/view` instead.

But, I was just reading the above and I realized that equation 4 isn't actually a problem. If we do it this way:

$$\sigma(1 \cdot \vec{a} + (-1) \cdot \vec{a}) = \sigma(\vec{a}) + \sigma(-\vec{a}) = \vec{a} + (-\vec{a}) = \vec{\emptyset}$$

it's still all fine. And, it's the same as if we do it this way.

$$\sigma(1 \cdot \vec{a} + (-1) \cdot \vec{a}) = 1 \cdot \sigma(\vec{a}) + (-1) \cdot \sigma(\vec{a}) = \vec{a} + (-\vec{a}) = \vec{\emptyset}$$

Index